★★事例 1★★

巧妙化するフィッシング詐欺

～本物そっくりの偽サイト～

Q1　偽メールによるフィッシング
　クレジットカード会社から【重要なお知らせ】「〇〇〇カードからの緊急のご連絡」というメールが来た。驚いてメールのリンクをクリックし、カード会社のサイトでカード情報や個人情報を入力したら、カードを不正利用されてしまった。

Q2　偽 SMS（※1）によるフィッシング
　宅配会社から「荷物をお届けしましたが不在のため持ち帰りました」という SMS が届いた。URL をタップしたら宅配会社のサイトのログイン画面になり、指示に従って ID やパスワードを入力したところ、自分のアカウントでサービスを不正利用されてしまった。

（※１）ショートメッセージサービスの略。電話番号を宛先に指定して、メッセージを送受信できる

　大手通販サイトやクレジット会社、宅配会社に加えて、通信事業者などをかたる偽メールや偽 SMS が増えています。誘導した偽サイトに個人情報を入力させて盗む「フィッシング詐欺」です。携帯電話会社の暗証番号などを入力させられ、キャリア決済（※2）を不正利用されたケースもあります。
　入力してしまった場合や、不正利用の被害に気付いた時は、すぐにカード会社など関係事業者に連絡して、調査を依頼してください。偽サイトに入力したカード番号やパスワードなどは、変更しましょう。

（※２）携帯電話会社の ID・パスワード・暗証番号などによる認証を利用することで、携帯利用料金と合算して商品等の購入代金を支払うことができる決済方法

★ワンポイント★

　偽サイトは巧妙に作られているので、見分けることは簡単ではありません。メールや SMS が本物かどうか迷った場合には、公式サイトなどで確認してください。日頃から、メールや SMS に記載された URL にはアクセスしないようにしましょう。クレジットカード番号、パスワード、暗証番号など、重要な情報は安易に入力しないように気を付けてください。
　フィッシングの手口はどんどん変化しています。最新の手口や対処方法は、（独）情報処理推進機構（IPA）、フィッシング対策協議会のホームページが参考になります。